



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/588,547	06/06/2000	TARO TERA0	106408	8229

25944 7590 02/07/2005

OLIFF & BERRIDGE, PLC  
P.O. BOX 19928  
ALEXANDRIA, VA 22320

EXAMINER
----------

KIM, JUNG W

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 02/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Advisory Action  
Before the Filing of an Appeal Brief**

Application No.

09/588,547

Applicant(s)

TERAO, TARO

Examiner

Jung W Kim

Art Unit

2132

**--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

THE REPLY FILED 26 January 2005 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☐ The period for reply expires \_\_\_\_\_ months from the mailing date of the final rejection.  
b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**NOTICE OF APPEAL**

2. ☐ The reply was filed after the date of filing a Notice of Appeal, but prior to the date of filing an appeal brief. The Notice of Appeal was filed on \_\_\_\_\_. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

**AMENDMENTS**

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because  
(a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);  
(b) ☐ They raise the issue of new matter (see NOTE below);  
(c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or  
(d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: See Continuation Sheet. (See 37 CFR 1.116 and 41.33(a)).

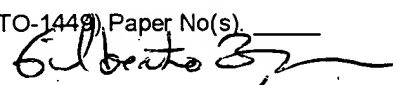
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).  
5. ☐ Applicant's reply has overcome the following rejection(s): \_\_\_\_\_.  
6. ☐ Newly proposed or amended claim(s) \_\_\_\_\_ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).  
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.  
The status of the claim(s) is (or will be) as follows:  
Claim(s) allowed: \_\_\_\_\_.  
Claim(s) objected to: \_\_\_\_\_.  
Claim(s) rejected: 1-38.  
Claim(s) withdrawn from consideration: \_\_\_\_\_.

**AFFIDAVIT OR OTHER EVIDENCE**

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).  
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).  
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

**REQUEST FOR RECONSIDERATION/OTHER**

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:  
See Continuation Sheet.  
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s) \_\_\_\_\_  
13. ☐ Other: \_\_\_\_\_

  
**GILBERTO BARRON JR.**  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

Continuation of 3. NOTE: proposed amendment to claims 1, 5, 7, 20, 21, 24, 25, 26, 28, 31, 33 introduces the limitations of a "right issuer"; a "unique value" calculation unit; u as a series of m values; creating by a hash value calculation unit; function  $X(M) = H(u_1|M) | \dots | H(U_m|M)$ ; "issuing a capability x ..."; "verifying the issuer ...."; "function generation unique value memory".

Continuation of 11. does NOT place the application in condition for allowance because: regarding applicant's argument the prior art of record does not teach features directed to "creating a value generation unique value u based on the user's unique value d and the function generation unique value s" (see pg. 16, 1st paragraph), examiner notes that the claimed features were actually directed to generating a one-way function dependent on a one-way function H and a unique value d for a user wherein the one-way function generates unique value u from the function generation unique value u and the unique value d, which is covered by Zhang, Walker and Wolfgang as outlined in the previous Office Action.

Regarding applicant's argument the prior art of record does not teach the feature of a tamper-resistant enclosure for a private key (see pg. 16, 2<sup>nd</sup> paragraph), examiner notes that an Official Notice was taken that a tamper-resistant enclosure for a private key are standard means of securing encryption keys.

Regarding applicant's argument no motivation to combine the features of Zhang, Walker and Wolfgang was given (see pg. 17, 1<sup>st</sup> paragraph), examiner disagrees and refers to the respective rejection of these claims in the previous Office Action.

In response to applicant's argument that the use conditions for message M is not analogous to use conditions within a certificate (see pg. 18, 1<sup>st</sup> full paragraph), it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, the use terms of a certificate dictate the policies that a value can be used or process; this is analogous to use terms to dictate how a message is used or processed. Further, both the prior art and the field of applicant's endeavor are within the cryptographic art.

In response to applicant's argument that the features of claim 11-14 have nothing in common with an encryption function with a symmetric key as the scrambling operation (see pg. 18, 2<sup>nd</sup> full paragraph), examiner notes that no such combination was made in the previous Office Action rejection to claims 11-14. See Office Action (Nov. 18, 2004), pgs. 13-14, paragraph 33.

In response to applicant's argument that the feature of updating the challenge c and/or the response r is unrelated to the necessity of showing equivalence between values, and hence, the prior art fails to teach the claimed limitation (see pg. 19, 1<sup>st</sup> full paragraph), examiner notes that such an argument does not respond to the extent of the rejection. The rejection states: although Zhang does not expressly disclose using the access ticket to update values used in authentication, these steps are obvious implementations for the following reasons: an access ticket expressed as a difference or a quotient of private key x and value X(M) are obvious constructions to show equality/inequality of two values as argued above in the claim 29 and 30 rejections, and further, the updates in claims 34-38 are obvious means to communicate the resulting discrepancy between x and X(M) to an authenticator in the authentication schemes as summarized by Schneier and listed above. As defined in the applicant's Specification (see expressions 65, 67, and 69 on page 48), the update procedure is defined by applying the following types of operations:  $z = z + z^*(x - X(M))$ ,  $z = z^*(x/X(M))$ , or  $z = z/(x/X(M))$ , wherein the z variable is a challenge or response value defined in a step of a conventional authentication scheme. In these cases, z remains the same if  $x == X(M)$ , and is updated to a different value if  $x \neq X(M)$ . Furthermore, as taught by Stallings, challenge or response approaches used in authentication methods typically comprise steps of submitting a value by a sender wherein the receiver is required to return the same value back to the sender (see Stallings, page 304, bullet 'Challenge/response'). Hence, the steps of claims 34-38 are simple variations of this theme. It would be obvious to one of ordinary skill in the art at the time the invention was made to update challenge or response values in step(s) of implemented authentication schemes to determine if a generated value is equivalent to a stored or received value and thus determine authentication. Motivation for such an implementation would use simple update functions to determine if authentication has succeeded or failed.

Regarding applicant's argument no motivation to combine the features of Zhang, Walker, Wolfgang, Stallings and Schneier was given (see pg. 20, 2<sup>nd</sup> full paragraph), examiner disagrees and refers to the respective rejection of these claims in the previous Office Action.

It is further noted that arguments pertaining to new limitations in the proposed amendments are not considered as they require new search and consideration.